



Slik får dere kontroll på bedriftens persondata

Den 25. mai 2018 trer de nye personvernreglene i kraft, også omtalt som GDPR - The General Data Protection Regulation.

Selskaper som ikke etterlever de nye reglene kan risikere bøter på opptil 20 millioner Euro, eller 4 % av selskapets globale omsetning dersom det tilsvarer en høyere sum.

De nye reglene vil ha stor innvirkning på hvordan bedrifter samler, behandler og bruker personlige data.

En del av det å etterleve personvernforordningen er å kartlegge hvor i organisasjonene personlige data oppstår/kommer fra. I tillegg må dere kartlegge hvor og hvordan dataene er lagret, og dokumentere hvordan dere bruker dataene.

Persondata kan være navn, adresse, telefonnummer, e-postadresse, IP-adresser, kjønn, inntekt, interesser og besøkte websider.

Mal for analyse av persondata

Denne listen med spørsmål kan benyttes som en start når dere skal analysere de personlige dataene dere har lagret i systemene deres.

Flere foretrekker å samle resultatene fra analysen i et Excel regneark slik at man har en oversikt ett sted. Men det er naturligvis mange andre måter dere kan samle disse datene på.

Det aller viktigste er at dere kan besvare og ha kontroll på disse 13 spørsmålene for hver type data dere lagrer.

- 1 Hva slags persondata er samlet inn?**

Angi en beskrivelse av hvilke typer informasjon som dere har samlet, for eksempel navn, adresse, e-post, telefonnummer. Ta også med mer personlig informasjon, så som fødselsdato, personnummer og andre opplysninger som identifiserer en person.
- 2 Hva er hensikten med å samle inn disse personlige opplysningene?**

Forklar hvorfor dere har innhentet denne informasjonen. Hvis dere virkelig trenger fødselsdatoen må dere forklare hvorfor og hva dere trenger denne informasjonen til.
- 3 Hva er det juridiske grunnlaget?**

Forklar selskapets lovmessige rett til å samle inn denne informasjonen. I personvernforordningens paragraf 6 er det angitt forskjellige lovmessige hjemler bedriften deres kan ha for å samle inn og bruke personlige opplysninger. Ekspisitt samtykke, kontrakt med brukeren, lovpålagte krav til bedriften og ivaretagelse av legitime interesser er slike grunner som kan være juridiske grunnlag. I dokumentasjonen må dere henvise til en eller flere av disse hjemlene i paragraf 6, og på den måten begrunne på hvilken måte deres praksis har støtte i personvernforordningen.
- 4 Hva er kilden til dataene med personlige opplysninger?**

Oppgi informasjon om hvordan dere skaffer til veie persondata. Får dere dem via webskjemaer, visittkort som samles inn i forskjellige sammenhenger, integrasjoner med andre systemer etc.?



5 Hva er klassifikasjonen?

Klassifikasjoner av persondata kan være konfidensielle, anonyme, sensitive etc. Informasjon om lønn og bonuser er for eksempel sensitive opplysninger. Husk at alle personlige opplysninger som er sensitive eller konfidensielle krever ekstra sikkerhetstiltak.

6 Hvor lenge blir de persondata lagret?

Notér ned hvor lenge dere vil besitte de personlige opplysningene. Tidsrammen dere planlegger for kan være avhengig av hensikten og det juridiske grunnlaget. For eksempel kan lønnsinformasjon oppbevares så lenge som regnskapsloven og arkivloven krever og gir tillatelse til.

7 Hvem kan få tilgang til persondataene?

Notér ned hvem som har tilgang til dataene. Her er noen eksempler: lønnspersonale kan få tilgang til personlige opplysninger i lønssystemet, HR-ansatte kan få tilgang til personalopplysninger, selgere kan få tilgang til kundeinformasjon.

8 Blir de personlige dataene overført til andre land?

Data med personlige opplysninger skal i utgangspunktet holdes innenfor EU. I andre tilfeller skal dere dokumentere om dataene overføres og med hvilken hensikt.

9 Hva slags system bruker dere for å lagre informasjonen?

Dere har mest sannsynlig separate systemer for lønn og kundeinformasjon. Dere må også dokumentere hvilket system som brukes for de enkelte personlige opplysningene. Dere trenger også å angi om systemene dere bruker er skybaserte.

10 Har dere innhentet eksplisitt samtykke til å bruke dataene?

Marker om personen frivillig har gitt dere hennes eller hans personlige opplysninger til bruk i markedskommunikasjon. Eksplisitt samtykke er spesielt viktig når dere lagrer og bruker informasjon om personer som dere ikke har et aktivt kundeforhold til.

11 Har personen blitt informert om at dere har informasjon om henne eller han?

Dette blir vanligvis beskrevet i en kundekontrakt, i et oppstartsmøte eller i en personvernerklæring på websiden deres

12 Blir persondata delt med tredjepart, og hvorfor?

Hvis dere deler persondata, må dere angi hvilken type informasjon dere deler med andre og hvilke tredjeparter som mottar disse opplysningene. Hvis dere bruker dataene til markedsføring, så må dere oppgi om dere viderefremidler personlige data med andre tredjeparter i personvernerklæringen og kontraktsdokumentene som regulerer kundeforholdene.

13 Hvordan er informasjonen sikret?

Beskriv sikkerhetstiltakene som beskytter de personlige opplysningene. Dette er spesielt viktig om dere lagrer sensitiv informasjon og dere er ansvarlige for at disse datene er forsvarlig sikret.

Hva gjør dere nå?

Når dere er gjennom denne listen vil dere også bli klar over hvilke data dere vil beholde. Det er en god ide å ikke bli sittende på flere opplysninger enn nødvendig, og kvitte seg med data som ikke blir brukt.

Hvis bedriften deres samler mye data uten hensikt og behov, så vil dere ikke kunne fortsette med det etter at personvernforordningen trer i kraft.

Å kartlegge bedriftens persondata og deretter bestemme hvilke data dere må beholde er de første viktige skrittene dere må ta for å kunne etterleve kravene i de nye EU-reglene.

Dere må også få på plass sikkerhetstiltak som beskytter de personlige opplysningene, og implementere gode rutiner for tilgang, sletting og arkivering av brukerdata.

Hvis du har spørsmål om hvordan SuperOfficer CRM kan støtte dere i arbeidet med å etterleve personvernforordningen, ikke nøl med å kontakte oss.

Merk: Innholdet i denne artikkelen er ikke å betrakte som juridiske råd og skal kun brukes i informasjonsøyemed.